AIONIQ®: the NDR platform

Behavioral and mapping analysis for Augmented Detection

GATEWATCHER

La détection des cybermenaces avancées : Nouveau défi des organisations

Les conséquences financières d'une cyberattaque peuvent fragiliser durablement votre organisation.

L'augmentation du volume des menaces complique l'évaluation de la criticité des alertes traitées par vos analystes.

La persistance d'une attaque ciblée sur votre SI non détectée peut aggraver le préjudice occasionné.

La complexité et la furtivité des dernières cyberattaques augmentent les risques de compromission de votre S.I.

3,86M$

représente le coût global moyen d'une violation de la sécurité des données en 2020. [1]

255%

d'augmentation du nombre d'attaques par rançongiciels en France entre 2019 et 2020. [2]

207 jours

en moyenne nécessaires à une entreprise pour détecter une brèche de sécurité sur son SI. [3]

53%

des intrusions réussies ne sont pas détectées par les outils de cyberdétection déjà en place. [4]

Aioniq®: Une analyse cartographique et comportementale des cybermenaces pour une détection augmentée offrant une visibilité inédite sur les attaques ciblées.

- **Détection des menaces, y compris en cas de flux chiffrés.** Aioniq® est une plateforme NDR capable d'identifier, grâce au machine learning, toutes menaces présentes au sein de votre infrastructure et ce même si vos flux de communication sont chiffrés.

- **Cartographie de l'intégralité des assets du SI** Aioniq® est la seule plateforme NDR capable de cartographier l'ensemble des actifs du SI de manière totalement passive et sans agent pour offrir un niveau de détection inédit des attaques avancées sur les flux est-ouest.

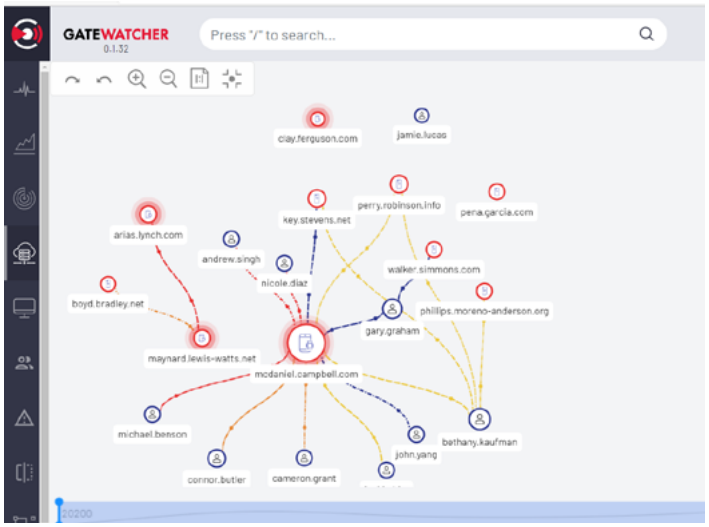
- **Meilleure visibilité sur les menaces dissimulées** Aioniq® est la seule plateforme NDR capable de fournir un niveau de détail et une typologie de métadonnées uniques sur le marché afin d'optimiser le temps nécessaire à vos analyses forensics.

- **Modélisation du risque par actif et utilisateur** Aioniq® est la seule plateforme NDR capable d'une modélisation Mitre Att&ck du niveau de compromission sur le SI associant évènement, asset et utilisateur avec une vision agrégée par risque de l'ensemble des alertes.

Aioniq® est une nouvelle plateforme de détection et de réponse (NDR) qui permet d'identifier avec certitude les actions malveillantes et les comportements suspects en s'appuyant sur une cartographie de l'intégralité des assets présents sur le SI.

L'association de cette capacité avec des performances inédites d'analyse des comportements malveillants, même en cas de flux réseau chiffrés, permet d'offrir une modélisation à 360° du niveau de risque cyber associé à chaque connexion entre assets et utilisateurs, pour un niveau de détection et de visibilité inégalé.

Granulaire et flexible, Aioniq® s'adapte en permanence pour offrir une réponse performante et personnalisée à toutes les cybermenaces, qu'elles soient connues et inconnue : Ransomwares, APTs, exploitations de vulnérabilités zero-day..



Sources : [1] Ponemon Institute, [2] ANSSI, [3] IBM, [4] FireEye Mandiant

Bénéfices utilisateurs

UNE PLATEFORME LOGICIELLE RESILIENTE AUX CYBERATTAQUES

Développé dans une approche de "Security by design", Aioniq® est doté d'un OS durci offrant une forte résistance aux tentatives de corruption et une surface d'attaque réduite.

UNE PROTECTION IMMÉDIATEMENT OPÉRATIONNELLE

Aioniq® n'implique pas d'équipements supplémentaires ou de coûts cachés. Paramétrable simplement Aioniq® détecte les menaces dès la phase d'audit et n'a aucun impact sur votre environnement de production.

UNE FORTE INTEROPÉRABILITÉ AVEC VOS ÉQUIPEMENTS

Aioniq® est une plateforme ouverte offrant une forte réactivité en cas d'attaque par sa connexion avec la plupart des outils de réponse et de remédiation du marché, EDR, SIEM, SOAR...

UNE OFFRE ALLIANT SCALABILITÉ ET PERFORMANCES

Aioniq® s'adapte aux spécificités de votre organisation ainsi qu'à la menace avec un système unique et évolutif de moteurs de détection. Avec une capacité de déploiement "on premise" ou dans le cloud.

UNE COUVERTURE GRANULAIRE ET FLEXIBLE

Aioniq® est disponible en plusieurs offres pour s'adapter parfaitement à votre infrastructure de protection et à vos choix technologiques afin de vous offrir une protection réellement sur-mesure.

UNE EFFICIENCE OPTIMISÉE DE VOTRE SOC

Par sa collecte de multiples métadonnées et sa cartographie avec visualisation chronologique des détections selon le référentiel MITRE ATT&CK, Aioniq® facilite l'investigation des analystes et la gestion de la criticité des alertes.

Cas d'usages

Détection: une utilisation raisonnée du machine learning. A la différence d'un modèle de détection recourant aveuglement à l'IA, Aioniq® se distingue par une approche multifactorielle composée d'analyse statique, dynamique et algorithmique en fonction de la typologie de la menace pour détecter les TTPs spécifiques à chaque cyberattaque.

- Détection de beaconing de type Cobalt Strike dans le cadre d'une attaque par DGA.
- Détection des anomalies réseaux dans des flux chiffrés.
- Détection de nouveaux algorithmes d'obfuscation utilisés dans des attaques est-ouest par mouvements latéraux.

Hunting: réagir aux premiers signes d'une attaque ciblée. Aioniq® est la seule solution du marché en mesure de couvrir l'intégralité de la Kill Chain d'une cyberattaque avancée et de repérer les technique d'exploitation utilisées tout au long de son déroulement.Les pirates n'ont plus d'endroit où se cacher.

- Investigation approfondie sur les types de metadonnées, les sessions, les protocoles et les actions utlisateurs.
- Gestion UEBA des interactions assets-utilisateurs permettant de se focaliser uniquement sur les risques principaux.
- Analyse a posteriori de l'ensemble des métadonnées avec des indicateurs de compromission de nouvelle génération.

Réponse à incident: une connexion fluide à vos outils pour une remédiation immédiate en cas d'attaque. Aioniq® est une solution agnostique et ouverte permettant de s'intégrer rapidement et harmonieusement dans la plupart des stacks de sécurité existants via un large catalogue d'API pour un réponse sans aucune latence en cas de cyberattaque.

- Capacité rapide de création de signatures personnalisées afin de s'adapter au contexte client.
- Automatisation SOAR de la réponse à incidents.
- Large choix d'API vers les EDR pour une réponse rapide et automatisée.

Forensique: une visibilité inédite sur les attaques pour une cyber résilience renforcée.
Les fonctionnalités offertes par Aioniq® en matiere de cartographie des assets et sa capacité à les relier à chaque utilisateur pour identifier le niveau de risque offre une visibilité post mortem inégalée sur le mode operatoire de chaque attaque.

- Collecte de multiples métadonnées permettant la contextualisation des attaques.
- Enrichissement rapide grâce aux interconnexion avec les différentes plateformes de Threat Intelligence du marché.
- Capacité d'investigation graphique interactive pour déterminer la chronologie et la propagation de chaque attaque.

A propos

Gatewatcher est un éditeur européen spécialisé dans la détection des cybermenaces et intrusions les plus avancées. Son modèle associe plusieurs technologies à l'I.A pour vous offrir une protection optimale.

Nous contacter

contact@gatewatcher.com
www.gatewatcher.com